

CLAIMS

WHAT IS CLAIMED IS:

1. A system, comprising:
a memory configured to store data; and
5 a device coupled to the memory, wherein the device includes a random number generator,
wherein the random number generator includes:
an entropy register configured to receive bits over a plurality of data lines, wherein
each of the plurality of data lines couples an individual entry in the entropy
register with a corresponding entry in another register.
10
2. The system of claim 1, wherein the random number generator further includes:
an entropy control unit configured to provide a value from the entropy register in
response to a request for a random number.
- 15 3. The system of claim 1, wherein the device further includes a plurality of registers,
wherein each of the plurality of data lines couples the individual entry in the entropy register
with a corresponding entry in one of the registers.
4. The system of claim 3, wherein the corresponding entry in the one of the plurality of
20 registers corresponds to the least significant bit entry in each of the plurality of registers.
5. The system of claim 3, wherein the plurality of registers include a plurality of
performance registers.
- 25 6. The system of claim 1, wherein the device includes a processor.

7. The system of claim 1, further comprising:

a bridge coupled between the memory and the device.

5 8. The system of claim 1, wherein the device is configured to cause data to be stored in the memory.

9. A device, comprising:

a random number generator coupled to receive signals from a plurality of bit lines, wherein

10 the random number generator includes:

an entropy register configured to receive bits over the plurality of data lines, wherein

each of the plurality of data lines couples an individual entry in the entropy

register with a corresponding entry in another register.

15 10. The device of claim 9, wherein the random number generator further includes:

an entropy control unit configured to provide a value from the entropy register in

response to a request for a random number.

11. The device of claim 9, further comprising:

20 the plurality of bit lines.

12. The device of claim 11, further comprising:

a plurality of registers, wherein each individual entry in the entropy register couples to

receive a signal from one of the plurality of data lines and to store a

25 corresponding entry in one of the plurality of registers.

13. The device of claim 12, wherein the corresponding entry in the one of the plurality of registers corresponds to the least significant bit entry in each of the plurality of registers.

14. The device of claim 12, wherein the plurality of registers include a plurality of performance registers.

15. The device of claim 9, wherein the device includes a processor.

16. A random number generator comprising an entropy register configured to receive bits over a plurality of data lines that each couple to an individual entry in the entropy register.

17. The random number generator of claim 16, further comprising:
an entropy control unit configured to provide a value from the entropy register in response to a request for a random number.

18. The random number generator of claim 16, further comprising:
the plurality of data lines.

19. The random number generator of claim 18, further comprising:
a plurality of registers coupled to the entropy register through the plurality of data lines, wherein each individual entry in the entropy register is coupled to one of the plurality of registers.

20. The random number generator of claim 19, wherein each of the plurality of data lines couples the individual entry in the entropy register with a corresponding entry in one of a plurality of registers.

5 21. The random number generator of claim 20, wherein the corresponding entry in the one of the plurality of performance registers corresponds to the least significant bit entry in each of the plurality of performance registers.

22. A method of generating a random number, the method comprising:
10 providing a first plurality of bit entries in an entropy register; and
transmitting a bit value from each of a plurality of registers to one of the first plurality of bit entries in the entropy register.

23. The method of claim 22, further comprising:
15 providing the bit values from each of the first plurality of bit entries in the entropy register.

24. The method of claim 23, further comprising:
receiving a request for a random number;
wherein providing the bit values from each of the first plurality of bit entries in the entropy
20 register comprises providing the bit values from each of the first plurality of bit entries in the entropy register in response to receiving the request for the random number.

25 25. The method of claim 24, wherein receiving the request for the random number includes receiving a length in bits for the random number, and wherein the length in

bits for the random number is less than or equal to a number of bit entries in the first plurality of bit entries.

26. The method of claim 24, further comprising:

- 5 prior to providing the bit values from each of the first plurality of bit entries in the entropy register,
- providing a control signal to the entropy register; and
- reading the bit values from each of the first plurality of bit entries in the entropy register.

10 27. A system, comprising:

a plurality of means for generating a first plurality of bits, wherein each of the plurality of means for generating the first plurality of bits generates one of the first plurality of bits;

15 means for storing the first plurality of bits;

means for providing the first plurality of bit entries to the means for storing the first plurality of bits; and

means for transmitting a bit value from each of plurality of means for generating the first plurality of bits to one of the first plurality of bit entries in the means for storing the first plurality of bits.

20 28. The system of claim 27, further comprising:

means for receiving a request for a random number;

means for providing the bit values from each of the first plurality of bit entries in the means

25 for storing the first plurality of bits in response to the request for the random number.

29. The system of claim 28, wherein said means for receiving a request for a random number is configured to receive a length in bits for the random number, and wherein the length in bits for the random number is less than or equal to a number of bit entries in the first plurality of bit entries in the means for storing the first plurality of bits.

30. The system of claim 28, further comprising:
means for providing a control signal to the means for storing the first plurality of bits; and
means for reading the bit values from each of the first plurality of bit entries in the means for storing the first plurality of bits;
wherein said means for providing the control signal and said means for reading the bit values are operable prior to said means for providing the bit values from each of the first plurality of bit entries in the means for storing the first plurality of bits.

31. A method for generating a random number, the method comprising:
step for providing a first plurality of bit entries; and
step for transmitting a bit value from each of a plurality of registers to one of the first plurality of bit entries.

32. The method of claim 31, further comprising:
step for providing the bit values from each of the first plurality of bit entries.

33. The method of claim 32, further comprising:

step for receiving a request for a random number;

wherein the step for providing the bit values from each of the first plurality of bit entries comprises step for providing the bit values from each of the first plurality of bit entries in response to the step for receiving the request for the random number.

5 34. The method of claim 33, wherein the step for receiving the request for the random number includes step for receiving a length in bits for the random number, and wherein the length in bits for the random number is less than or equal to a number of bit entries in the first plurality of bit entries.

10 35. The method of claim 33, further comprising:
prior to the step for providing the bit values from each of the first plurality of bit entries,
step for controlling the first plurality of bit entries; and
step for reading the bit values from each of the first plurality of bit entries.

15 36. A computer readable program storage device encoded with instructions that, when executed by a computer, performs a method of generating a random number, the method comprising:

20 providing a first plurality of bit entries to an entropy register; and
transmitting a bit value from each of a plurality of registers to one of the first plurality of bit entries in the entropy register.

37. The computer readable program storage device of claim 36, the method further comprising:

providing the bit values from each of the first plurality of bit entries in the entropy register.

25

38. The computer readable program storage device of claim 36, the method further comprising:

receiving a request for a random number;

wherein providing the bit values from each of the first plurality of bit entries in the entropy

5 register comprises providing the bit values from each of the first plurality of bit entries in the entropy register in response to receiving the request for the random number.

39. The computer readable program storage device of claim 38, wherein receiving the request for the random number includes receiving a length in bits for the random number, and wherein the length in bits for the random number is less than or equal to a number of bit entries in the first plurality of bit entries.

40. The computer readable program storage device of claim 38, further comprising:
prior to providing the bit values from each of the first plurality of bit entries in the entropy register,
providing a control signal to the entropy register; and
reading the bit values from each of the first plurality of bit entries in the entropy register.